ATITALAQUIA
SE TRANSFORMA
2024-2027

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL MUNICIPIO DE ATITALAQUIA, HIDALGO

2025

ATITALAQUIA
SE TRANSFORMA
2024-2027

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Ayuntamiento Constitucional de Atitalaquia 2024-2027

Mtro. José Edgardo León García
Titular de la Unidad Municipal de Transparencia
del muncipio de Atitalaquia

Municipio de Atitalaquia, Hgo.

CONTENIDO

INTRODUCCIÓN....4
OBJETIVOS 6
CONCEPTOS BASICOS....6
OBJETIVOS ESPECIFICOS DEL DOCUMENTO DE SEGURIDAD 9
RESPONSABILIDADES 10
MARCO NORMATIVO 10
SISTEMAS DE GESTIÓN DE DATOS PERSONALES....11
CATÁLOGO, DESCRIPCIÓN Y MEDIDAS DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES DEL AYUNTAMIENTO DE ATITALAQUIA 11
CONTROLES Y MECANISMOS DE SEGURIDAD....15
LAS BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA, Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES....16
ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA 17
GESTIÓN DE VULNERACIONES....19
MEDIDAS DE SEGURIDAD APLICADAS A LAS INSTALACIONES. 20
LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN A LAS INSTALACIONES. 23
LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES....23
EL PLAN DE TRABAJO Y PROGRAMA GENERAL DE CAPACITACIÓN....23
MECANISMOS DE MONITOREO Y REVISIÓN DE MEDIDAS DE SEGURIDAD....24
CONCLUSIONES....25

INTRODUCCIÓN.

Durante los últimos años, la protección de los datos personales se ha convertido en un tema de vital importancia para los individuos, las empresas y los gobiernos en todos los niveles. La protección de datos personales es una medida que tiene como objetivo garantizar la privacidad y seguridad sobre los datos personales de una persona, en línea o en cualquier otro medio.

La protección de datos personales se refiere al conjunto de medidas y prácticas que tienen como objetivo proteger la privacidad de las personas y garantizar que sus datos personales sean utilizados de manera responsable y ética. Estos datos incluyen información como nombres, direcciones, números de teléfono, direcciones de correo electrónico, información financiera y de salud, entre otros.

A decir verdad, en la mayoría de los municipios en el Estado de Hidalgo aún se registran atrasos importantes en materia de protección de datos personales, las razones pueden ser variadas, desde falta de personal hasta falta de recursos e interés por parte de las autoridades, lo que resulta cierto es que hace falta dar pasos ágiles, firmes y estratégicos que nos permitan avanzar en el camino correcto en materia de protección de datos personales.

Por tanto, la importancia de la protección de datos personales radica en varios aspectos.

En primer lugar, la privacidad es un derecho fundamental que debe ser protegido. Todos tenemos derecho a decidir qué información compartimos y con quién la compartimos. Cuando se recopilan datos personales sin nuestro conocimiento o consentimiento, se viola nuestra privacidad y se pone en riesgo nuestra seguridad.

En segundo lugar, los datos personales son valiosos y pueden ser utilizados con fines malintencionados. La información financiera y de identificación personal puede ser mal utilizada, para cometer cualquier tipo de delito. La información personal también puede ser utilizada para acosar o amenazar a las personas.

En tercer lugar, la pérdida o el robo de datos personales puede tener consecuencias graves, como las violaciones a los derechos humanos, interrupción de los sistemas de seguridad y el rompimiento de relaciones entre clientes e inversores o incluso la pérdida de confianza entre usuarios internos y externos en el ámbito gubernamental.

Por todas estas razones, es importante que se adopten medidas de protección de datos personales. Los gobiernos sobre todo deben implementar políticas y prácticas que garanticen la privacidad y la seguridad de los datos personales. Esto incluye medidas como la implementación de protocolos de seguridad para proteger los datos, la educación de los empleados y los usuarios sobre las mejores prácticas de seguridad, y la adopción de leyes y regulaciones que protejan los datos personales y establezcan sanciones para aquellos que los violen.

La Unidad Municipal de Transparencia del municipio de Atitalaquia, Hidalgo, reconoce el Derecho Humano de la protección de datos personales, establecido en la Constitución Política de los Estados Unidos Mexicanos en los artículos 6, apartado A, fracciones II y III y 16, segundo párrafo.

A partir de la reforma constitucional de 2009, la protección de datos personales quedó establecida como un derecho fundamental, el cual reconoce que toda persona tiene derecho a la protección, y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales. Reconocidos también como derechos ARCO.

El 24 de julio de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo, que tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados.

En diciembre de 2024, México emprendió una reforma constitucional significativa en materia de protección de datos personales, que culminó con la publicación de nuevas leyes secundarias en marzo de 2025. Esta reforma implicó la eliminación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), redistribuyendo sus funciones entre otras instancias gubernamentales. El objetivo principal fue fortalecer la transparencia y la seguridad de los datos personales, optimizando recursos y mejorando la eficiencia institucional.

Para la ciudadanía, estas reformas representan un cambio sustancial en la forma en que se garantiza el derecho a la privacidad. Se han establecido principios más estrictos sobre el consentimiento, la finalidad del tratamiento de datos y la calidad de la información recopilada. Además, se han reforzado los mecanismos de seguridad para evitar el uso indebido de datos personales por parte de empresas, organizaciones y entidades públicas. Esto genera mayor confianza en el manejo de información sensible, especialmente en un contexto de creciente digitalización.

A nivel municipal, los gobiernos locales como el de Atitalaquia enfrentan nuevos retos y responsabilidades. Las reformas exigen una actualización de los sistemas de gestión de datos, capacitación del personal en normativas vigentes y la implementación de protocolos más rigurosos para el tratamiento de información personal. Asimismo, se espera una mayor coordinación con instancias estatales y federales para garantizar el cumplimiento de los nuevos estándares, lo que convierte a la protección de datos en un eje transversal de la administración pública municipal.

En tal virtud, la Unidad de Transparencia en estricto apego a las disposiciones que en materia dispongan la protección de datos personales deberá observar en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad; así como los deberes de seguridad y confidencialidad.

Dichos principios y deberes dictan una serie de obligaciones de observancia para los responsables, que tiene como propósito que el tratamiento se realice garantizando la protección de los datos personales de sus titulares.

En relación con el deber de seguridad, se presenta el Documento de Seguridad de Datos Personales en el que se establecen las medidas de seguridad de carácter administrativo, físico y técnico que se han adoptado para el adecuado tratamiento de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado a través del ciclo de vida de los datos personales; así como garantizar su confidencialidad, integridad y disponibilidad.

OBJETIVOS

El presente instrumento cuenta con los objetivos siguientes:

- Describir las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Unidad Municipal de Transparencia para garantizar la confidencialidad, integridad y disponibilidad de los datos personales;
- Detallar los mecanismos establecidos para supervisar, monitorear y auditar a las instancias que realicen el tratamiento de datos personales en la administración pública municipal;
- Evidenciar el cumplimiento de los principios y deberes previstos para la protección de datos personales en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo en general y, en lo particular, el deber de seguridad;

Su comprensión permitirá que cualquier persona interesada:

- Conozca las medidas de seguridad técnicas, físicas y administrativas implementadas por las instancias que realizan el tratamiento de datos personales;
- Se advierta la forma en que deben ser ejecutados los mecanismos dispuestos para la supervisión, monitoreo y auditoría de las instancias que realizan el tratamiento de datos personales;
- Se informe de la manera en que la Unidad Municipal de Transparencia, documenta el cumplimiento del deber de seguridad y con ello, como garantiza la confidencialidad, integridad y disponibilidad de los datos personales.

CONCEPTOS BASICOS.

Para los efectos del presente documento, se ha elaborado un listado de conceptos básicos para su mejor comprensión y que se presenta a continuación:

Aviso de privacidad: Documento legal que informa a las personas sobre cómo se recopilan, usan, almacenan y protegen sus datos personales. Este documento debe ser proporcionado por la unidad administrativa al momento de recabar los datos y detalla, entre otras cosas, la identificación del responsable, las finalidades del tratamiento, el tipo de datos recabados y cómo ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO). Su objetivo principal es permitir que los individuos tomen decisiones sobre su información y mantengan el control sobre ella.

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u organización

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos Biométricos. Son los datos personales relacionados con las características físicas, fisiológicas o de comportamiento de una persona física, que permite o confirma la identificación única de la misma. De manera enunciativa más no limitativa, son considerados datos biométricos, la huella dactilar, el reconocimiento facial, vascular, de iris o retina; y la geometría de la mano u oreja.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género;

Derechos ARCO: Los derechos de acceso, rectificación y cancelación de datos personales, así como la oposición al tratamiento de los mismos.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad a nivel organizacional, identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades.

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable sus instalaciones físicas, áreas críticas, recurso y datos personales.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales.

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del responsable.

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Los sistemas de datos personales se distinguen en:

a) **Físicos:** Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.
b) **Automatizados:** Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Soporte electrónico: Son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos, es decir, cintas magnéticas de audio, vídeo y datos, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, demás análogos.

Titular: La persona física a quien correspondan los datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión,

almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de datos personales.

Unidad Municipal de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Vulneración de datos personales: Es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

OBJETIVOS ESPECÍFICOS DEL DOCUMENTO DE SEGURIDAD

Garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad necesarias para la protección de los mismos y el cumplimiento de las obligaciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

En su artículo 48[1]. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares; y
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
III. Elaborar un inventario de los datos personales y de las bases y/o sistemas de tratamiento;
IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

[1] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y

VIII. Diseñar y aplicar diferentes niveles de capacitación de su personal, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

RESPONSABILIDADES

En apego al Artículo 117[2] es responsabilidad del Comité de Transparencia las siguientes funciones:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;

II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;

III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO;

V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y demás ordenamientos que resulten aplicables en la materia;

VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VII. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto;

VIII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

IX. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

MARCO NORMATIVO

- Constitución Política del Estado Libre y Soberano de Hidalgo,
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo,

[2] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo,
- Lineamientos para la Clasificación-Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

SISTEMAS DE GESTIÓN DE DATOS PERSONALES.

El Sistema de Gestión de Datos Personales es el medio por el cual la Unidad Municipal de Transparencia del municipio de Atitalaquia, Hidalgo, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo y en atención a lo dispuesto en su artículo 53, los elementos quedan contenidos en la siguiente tabla y apartados siguientes para quedar como sigue:

CATÁLOGO, DESCRIPCIÓN Y MEDIDAS DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES DEL AYUNTAMIENTO DE ATITALAQUIA

II. Nombre, cargo y adscripción	III. Funciones y Obligaciones	I. Nombre del Sistema de Tratamiento de Datos Personales	IV. Inventario de datos personales	VII. Tipo de soporte y características donde se resguardan
Lic. Lizbeth Anel Alpizar Tapia Secretaria General Municipal	Elaboración de actas de las sesiones del pleno; Realizar al término de su empleo, cargo o comisión el acta entrega recepción con la intervención de la Contraloría Municipal para la entrega de los recursos humanos, material es, documentación y asuntos sustantivos en trámite etc.	Actas de sesiones de las Comisiones especiales y permanentes	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
		Actas de sesiones del pleno del Ayuntamiento		
		Acta de entrega recepción		
LD. Ana Laura Neri Martínez Titular de la Contraloría Municipal	Implementar las normas de control, fiscalización, contabilidad y auditoría que deben observar las dependencias, órganos, organismos descentralizados municipales, previa consulta con la Auditoria Superior del Estado y la Secretaría de Contraloría de la Administración Pública Estatal;	Registro de quejas, denuncias y sugerencias.	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta baja, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
		Actas de entrega recepción		
		Declaraciones patrimoniales		
		Informes de presunta responsabilidad administrativa		
		Informes de auditoría y pliegos de recomendación		

		Informes de auditoría externa		
Lic. Rosa Margarita Basurto Secretaria Ejecutiva SIPINNA	Recibir a través de la unidad de primer contacto quejas y denuncias por violaciones a los derechos contenidos en la Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Hidalgo y demás disposiciones aplicables, así como canalizarlas de forma inmediata a la Procuraduría de Protección de Niñas, Niños, adolescentes y la Familia del Estado de Hidalgo, sin perjuicio que ésta pueda recibirla directamente	Elaboración de reportes Seguimiento a los Planes de protección y acción de la unidad de primer contacto	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Sistema DIF Municipal, planta baja, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
LP. Eva Ofelia Díaz Ríos Titular de la Instancia Municipal para el Desarrollo de las Mujeres	Apoyar a mujeres en situaciones de riesgo, víctimas de maltratos y violencia; Establecer programas, proyectos, defensa y cumplimiento de los derechos de las mujeres de manera integral y permanente en el municipio, en observancia dentro del plan municipal de desarrollo	Programas de apoyo a mujeres en situaciones de riesgo. Programas de defensa de los derechos de las mujeres.	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Sistema DIF Municipal, planta baja, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
LD. Carlos Eduardo Bejarano Dirección Jurídica	Asesoría, revisión y en su caso elaboración de contratos, acuerdos y convenios en los que participe o intervenga el Ayuntamiento o las dependencias de la administración pública Municipal. Formular los informes previos y justificados para los incidentes de suspensión y los juicios de amparo, respectivamente, que los particulares presentan en contra de actos de las distintas autoridades municipales, en los asuntos que le instruya el Presidente Municipal y Sindicatura Jurídica.	Contratos, acuerdos y convenios en los que participe o intervenga el Ayuntamiento Informes previos y justificados para los incidentes de suspensión y los juicios de amparo	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
MGP. José Edgardo León García Unidad Municipal de Transparencia y Acceso a la Información	Recibir y dar trámite a las solicitudes de acceso a la información Recabar y difundir la información a que se refieren los artículos 69 y 70 de la Ley de Transparencia y propiciar que las áreas la actualicen periódicamente, conforme la normatividad aplicable;	Respuesta a solicitudes de información de acceso y de datos personales Cumplimiento a las obligaciones de Transparencia a través del SIPOT y del Portal Oficial	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.

Lic. Blanca Esthela Camargo Ángeles Dirección de Comunicación Social y Soporte Técnico	Diseñar y elaborar estrategias de contenidos, definiendo aspectos previamente como: ¿A quién se le va hablar?, ¿qué se va a decir?, tipos de palabras claves y elegir la información para redes sociales o medios periodísticos.	Análisis de contenido	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
Lic. Lizbeth Anel Alpizar Tapia Secretaria General Municipal	Expedir las copias, credenciales y demás certificaciones y documentos que acuerde el presidente municipal. Implementar los mecanismos de comunicación y organización entre el gobierno municipal y las comunidades, procurando que éstos sean adecuados, oportunos y eficientes. Conocer, calificar e imponer las sanciones administrativas que procedan por faltas e infracciones al Bando Municipal, reglamentos y demás disposiciones de carácter general, generando así el acuerdo de retención; Coordinar la operación de los archivos de trámite, concentración e histórico, de acuerdo con la normatividad; Recepción de documentos y elaboración de cartillas de identidad militar	Tramite de constancias para la ciudadanía Elección de delegados Sanciones por faltas administrativas Resguarda de los archivos de trámite, concentración e histórico Expedición de cartilla de identidad militar Resguardo, respaldo y digitalización de la información	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
LC. Benito Hernández Cerón Tesorero Municipal	Elaborar y proponer estrategias para una mejor captación de ingresos; así como, presentar aquellas que contribuyan a fomentar la cultura de pago en los contribuyentes, Vigilar, supervisar y administrar la correcta aplicación del Presupuesto de Egresos autorizado, de conformidad con los programas y proyectos establecidos por las unidades administrativas Registro de apoyos otorgados, Integrar toda la información con relación a sueldos y salarios, prestaciones, compensaciones Supervisar el registro contable, presupuestal, funcional y programático de ingresos y egresos de todos los fondos de libre disposición y federales etiquetados	Estrategias de recaudación Programas y/p proyectos de las unidades administrativas. Apoyos a comunidades Dispersión de nomina Registros contables de egresos e ingresos de fondos y propios	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
Ing. Jonathan Josué Sandoval Montoya Dirección de Obras Públicas	Vigilar que la planeación, programación, presupuestación, adjudicación, contratación, ejecución, conservación, mantenimiento, demolición, gasto y control de las obras públicas que deba realizar el Ayuntamiento; Previo pago de derechos, Expedir permisos o licencias para la demolición, construcción, ampliación o remodelación de casas, edificios, banquetas, bardas, conexiones de drenajes y otros análogos; Emitir órdenes de pago de las constancias en el área de cajas de la secretaría de tesorería municipal;	Programación anual de obra pública Licencias de construcción Expedición de permisos y constancias en materia de ordenamiento urbano	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta alta, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.

LC. Anahí Hernández Ángeles Directora de Planeación y PbR	Dar seguimiento a la difusión y publicidad de los resultados, de las evaluaciones y seguimiento de los Aspectos Susceptibles de Mejora; Promover la integración y ejecución de los programas de alto impacto, para atender las necesidades específicas del municipio de Atitalaquia.	Difusión y publicidad de resultados Integración de programas	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP),	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, (anexo planta alta), espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
Lic. José Antonio Trejo Rodríguez Dirección de Desarrollo Social	Identificación de proyectos y/o programas con base a las necesidades inmediatas dé cada comunidad, observando las reglas de operación de los mismos para su formulación y operación; Establecer los lineamientos, normas y políticas mediante las cuales la dirección proporcionara informes, datos y cooperación técnica cuando le sea requerida por alguna otra área correspondiente; Identificar los programas sociales de los tres órdenes de gobierno, así como apoyos sociales del sector privado para beneficio social; Promover y garantizar el registro del mayor número de la población Atitalaquense perteneciente a los grupos vulnerables a programas federales existentes.	Padrón de los programas sociales de los tres órdenes de gobierno	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Datos como el estado físico o mental, cualquier atención médica, expediente clínico, diagnósticos, padecimientos, vacunas, intervenciones quirúrgicas, incapacidades médicas, discapacidades, uso de aparatos oftalmológicos, ortopédicos, auditivos o prótesis, consumo de sustancias tóxicas y estupefacientes, sintomatologías o análogos relacionados con nuestra salud	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, (anexo planta alta), espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.
Cmdte. Luis Felipe Mera Hernández Director de Seguridad Pública, Tránsito Municipal	Verificar la información generada por la policía de gabinete (plataforma México) para la realización de los operativos en el combate a la incidencia delictiva; Intervenir en situaciones de violencia familiar, en coadyuvancia con las autoridades competentes, en la observancia y cumplimiento de las leyes; Canalizar ante las instancias correspondientes a las personas víctimas de violencia, brindando acompañamiento en todo momento; Verificar el cumplimiento del personal a su cargo en las actividades relacionadas con el informe policial homologado, así como la entrega oportuna del mismo a la unidad de análisis. Llevar a cabo los lineamientos de Presentación, interrogatorio, revisión, análisis y emitir un dictamen de las condiciones en las que se encuentra la persona	Base de datos de la Plataforma México Base de datos sobre situaciones de violencia familiar Base de datos sobre situaciones de violencia Base de datos relaciona con el informe policial homologado Lineamientos de Presentación y emitir un	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas de Seguridad Pública Municipal, Av. Insurgentes S/N, Col Centro, Atitalaquia, Hidalgo, planta baja, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado

	que fue retenida por alguna falta dentro de los lineamientos judiciales vigentes de Seguridad pública y tránsito municipal; Recibir y atender quejas y denuncias, así como realizar las investigaciones, relacionadas con actos irregulares y de corrupción de la actuación policial, proponiendo medidas y acciones para inhibirlos; Ejercer inspección, control y vigilancia en materia de protección civil en los establecimientos del sector público, privado y social para prevenir alguna contingencia; Recabar información del servicio (fecha, hora, nombre de quien reporta, edad, lugar, requisitar solicitud de combustible con los servicio y sello del lugar, FRAP (ambulancia);	dictamen de las condiciones en las que se encuentra la persona que fue retenida por alguna falta Base de datos sobre quejas y denuncias Padrón de establecimientos, púbicos, privados y sociales	Datos como el estado físico o mental, cualquier atención médica, expediente clínico, diagnósticos, padecimientos, vacunas, intervenciones quirúrgicas, incapacidades médicas, discapacidades, uso de aparatos oftalmológicos, ortopédicos, auditivos o prótesis, consumo de sustancias tóxicas y estupefacientes, sintomatologías o análogos relacionados con nuestra salud	y previa identificación.
Lic. José Antonio Trejo Rodríguez Director de Desarrollo Económico	Implementar proyectos, programas y acciones que incentiven el desarrollo, la modernización, competitividad y crecimiento de los sectores productivos del Municipio, brindando especial atención a las micro, pequeña y mediana empresa propiciando su articulación productiva y la canalización oportuna de los apoyos, estímulos e incentivos que prevé la legislación aplicable en la materia; Administrar el Registro de Trámites y Servicios; Proponer y dar seguimiento a metodologías para la organización y sistematización de la información administrativa y estadística, así como los indicadores que deberán adoptar los Sujetos Obligados en materia de Mejora Regulatoria; Generar propuestas encaminados a que los trámites municipales requeridos para obtener una licencia para la apertura de empresas de bajo riesgo se realicen en el mismo lugar; Vinculación de buscadores de empleo con empresas, mediante la publicación de la oferta de vacantes laborales en el sector económico y creación de estrategias de vinculación laboral.	Padrón de programas de desarrollo de los sectores productivos Padrón de registro de trámites y servicios Programa de sistematización de información administrativa Padrón de trámites para la obtención de licencias de apertura de empresas Padrón de vinculación	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), nombres de familiares, dependientes y/o beneficiarios	Físico: consistente en documentos y expedientes. Electrónico consistente en hojas de cálculo y bases de datos relacional. Oficinas del Palacio Municipal, planta baja, espacio adecuado, bien ventilado y seco, con accesos restringidos para personal autorizado y previa identificación.

Fuente: Con base en el Manual de Organización de la Administración Pública Municipal 2021-2024, vigente, publicado el 13 de abril del 2021. https://www.atitalaquia.gob.mx/TRANSPARENCIA-69-nuevo/02-estructura-organica/2021-1/MANUAL-DE-ORGANIZACION-INSTITUCIONAL-ATITALAQUIA.pdf

CONTROLES Y MECANISMOS DE SEGURIDAD.

Cuando hablamos de los mecanismos de monitoreo y revisión de las medidas de seguridad en protección de datos personales, se refiere a todas las acciones, actividades, instrumentos, herramientas, controles o mecanismos administrativos, técnicos y físicos que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso o acceso no autorizado, garantizando con ello la confidencialidad, integridad y disponibilidad de los datos personales. Se identifican las medidas de seguridad a continuación se describen las medidas comunes.

1. **Medidas de seguridad administrativas:** Acciones y mecanismos implementados en el tratamiento de datos personales a nivel organizacional, como lo son las políticas y procedimientos para la gestión y revisión de la seguridad de la información, identificación, clasificación y borrado seguro de la información, así como sensibilización y capacitación del personal, en materia de protección de datos personales.

2. **Medidas de seguridad físicas:** Acciones y mecanismos para proteger el entorno físico, instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

3. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología y los recursos involucrados en su tratamiento.

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

LAS BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Bitácoras de Acceso.

Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:

- Nombre y cargo de quien accede,
- Identificación del Expediente,
- Fojas del Expediente,
- Propósito del Acceso,
- Fecha de Acceso,
- Hora de Acceso,
- Fecha de Devolución,
- Hora de Devolución.

Bitácoras de Vulneración de los Datos Personales.

La bitácora de vulneraciones contiene la siguiente información:

- Nombre de quien reporta el incidente,
- Cargo,
- La fecha en la que ocurrió;
- El motivo de la vulneración de seguridad; y
- Las acciones correctivas implementadas de forma inmediata y definitiva.

ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA

Análisis de riesgos: Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se ha logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

1) Obtención de datos incompletos o incorrectos.

2) Omitir la notificación al titular de los datos personales del aviso de privacidad.

3) No difundir el aviso de privacidad.

4) No tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad, por no tener un consentimiento expreso.

Después de identificar dichos riesgos es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del municipio.	Adquirir información o datos personales	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del municipio. Extorsiones.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Ataques a personas, robo de información, vulneración a la seguridad física y mental de los ciudadanos, robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales. Ataque a otros servidores públicos. Robo de información.	Obtener información para beneficio personal, curiosidad, error involuntario, por fines económicos.	Pérdida de datos personales, uso indebido de datos personales, uso ilícito de datos personales, robo de información, extorsión, modificaciones no autorizadas, robo de información.
Daño físico.	Agua, fuego, accidentes, corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos, fenómenos meteorológicos, sismos.	Cualquier eventualidad por causa natural, daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad, falla o pérdida de internet, falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales, divulgación y

		transferencia de datos personales, modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente, falla en equipos.	Poca o absoluta renovación de equipos de telecomunicaciones o cómputos, cambios de voltaje, pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas, falta de mecanismos para identificar o autenticación de usuarios, falta de actualización de antivirus	Pérdida, destrucción y daño, divulgación y transferencia de datos personales, modificaciones no autorizadas, robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño, divulgación y transferencia de datos personales, modificaciones no autorizadas, robo de información.
Espacio donde se archiven.	Carencia de espacio, espacio con poca seguridad, espacio no adecuado, falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales, divulgación y transferencia de datos personales, modificaciones no autorizadas, robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales, la falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Análisis de brecha: *Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, se puede realizar el análisis de brecha, utilizando como base la experiencia comentada por los servidores públicos de las unidades administrativas generadoras de información a la Unidad Municipal de Transparencia, como resultado de ello se identificaron las medidas de seguridad preexistentes:*

- *Quién recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.*
- *El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.*
- *Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.*
- *En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los*

ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.

- Cada oficina cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada está en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente por los titulares y unidades administrativas del sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

GESTIÓN DE VULNERACIONES

1) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos;

2) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes;

3) Recuperación de las Bitácoras de Acceso y de Vulneración de los Datos Personales;

4) Determinar responsables;

5) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares;

6) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad Municipal de Transparencia;

7) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales;

8) Notificar mediante oficio, al Instituto de Transparencia, Acceso a la información y Protección de Datos Personales del Estado de Hidalgo, para que determine lo conducente.

MEDIDAS DE SEGURIDAD APLICADAS A LAS INSTALACIONES.

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

En relación a lo anterior se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo de control	Descripción
Control de servidores públicos que recaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. (Quién recabe los datos generales para el trámite a realizar). Actualización del listado: cada 6 meses.
Control de servidores públicos que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales impartida por la Unidad Municipal de Transparencia
	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Obtención de datos.	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad.	El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite. Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del instituto, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, ésta deberá contener la mención y debe

	dar a conocer el aviso de privacidad del Instituto, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general.
Espacio físico.	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área. El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones. Las llaves de las puertas de cada dependencia, deberán ser guardadas únicamente por servidores públicos del área, autorizados para poseer las llaves. Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados. Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado
Resguardo provisional, durante el desahogo del trámite.	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.
Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: • No estar al alcance de los ciudadanos o servidores públicos ajenos al área. • Deberá ser un área específica para guardar los expedientes. • Este archivo debe estar bajo llave. • La llave del mismo solo puede estar en manos de un servidor autorizado para esto.
Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener lo siguiente: • Registro para anotar el nombre y puesto del servidor público autorizado. • Fecha, hora de entrada y hora de salida del archivo. • Registrar el expediente que se consultó. • Registrar el expediente que se extrae del archivo, y fecha en la que se regresa el expediente. • Firma de conformidad del servidor público que entró. • Firma de consentimiento del servidor público autorizado para llevar el control de este archivo.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal.

	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera semestral.
Inventarios Documentales.	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos. Esto es, un inventario de documentos que se mandan al Archivo Municipal para su resguardo.
Transferencia de datos personales.	En caso de ser necesario y derivado de las funciones de los servidores públicos, o por requisito del trámite, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública.

Medidas de seguridad para transferencias: las transferencias al interior del sujeto obligado y a otros sujetos obligados:

1) Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.

2) El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.

3) El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.

4) El área o dependencia gubernamental que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.

5) El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.

6) El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales tratándose de procedimientos de derecho ARCO.

7) Notificar mediante oficio, a la Unidad de Transparencia, la transferencia de datos personales, la finalidad, el medio y la unidad administrativa o dependencia gubernamental a quienes fueron transferidos.

Medidas de seguridad en caso de vulneraciones a la seguridad: en caso de ocurrir alguna vulneración deberá registrarse en la bitácora de vulneraciones, aclarando la fecha en la que ocurrió y las acciones correctivas implementadas de forma inmediata y definitiva.

LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN A LAS INSTALACIONES.

Los servidores públicos trabajadores de la Administración Pública Municipal de Atitalaquia, Hidalgo en todo momento deberán portar gafetes identificativos, los cuales deberán al menos contener:

- Nombre,
- Área de adscripción,
- Fotografía,
- Vigencia,
- Número de empleado,
- Firma del Secretario General Municipal,
- Domicilio institucional,
- Teléfono institucional.

LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que es probable su exposición, se aplicaran las medidas de seguridad tratadas anteriormente, mismas que están sujetas a cambios por eventualidades no contempladas.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos que día a día evoluciona.

EL PLAN DE TRABAJO Y PROGRAMA GENERAL DE CAPACITACIÓN.

Para la máxima protección de datos personales, debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad del plan es plasmar de manera enunciativa, más no limitativa, las actividades que la Unidad Municipal de Transparencia realizará para la aplicación del presente documento de seguridad, lo anterior se realizará en base a las atribuciones establecidas en la Ley de Protección de Datos Personales en Posesión de sujetos Obligados para el Estado de Hidalgo.

1) Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.

2) Se comunicará a los servidores públicos designados por sus titulares la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

3) Se buscará la participación del ITAIH, para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará cada 6 meses, a partir de la emisión del presente documento de seguridad:

1) Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado,

2) Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para la Administración Pública Municipal.

3) Actualizar el presente plan de trabajo.

4) Se emitirá un programa anual de capacitaciones y además se promoverá que el personal de la Administración Pública Municipal se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

Estrategias de capacitación	
Capacitación permanente (una vez aprobado el Manual de Organización y de Procedimientos, dado que el vigente se encuentra desactualizado)	Ofrecer cursos sobre aspectos generales de la Ley de Protección de Datos Posesión de Sujetos Obligados del Estado de Hidalgo
Capacitación focalizada (Una vez al mes, o bien cuando sea requerido por la Unidad Administrativa).	Se impartirá los cursos específicos acorde a las necesidades de la Unidades Administrativas y Áreas Generadoras de la Información.
Acciones de capacitación a responsables de tratamiento	
Proporciona a los servidores públicos las herramientas necesarias que les permitan mejorar la gestión de la protección de datos personales a fin de incrementar los niveles de seguridad en el tratamiento de datos personales al interior de la institución.	
Impartido por: Unidad Municipal de Transparencia. Dirigida a: Integrantes del Comité de Transparencia, titulares de las unidades administrativas, y cualquier otro personal involucrado en el tratamiento de datos personales al interior de la institución.	Curso: Aspectos Generales de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. Curso: Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Hidalgo Curso-taller: Derechos ARCO Taller: Documento de Seguridad Taller: Elaboración de Avisos de Privacidad.

MECANISMOS DE MONITOREO Y REVISIÓN DE MEDIDAS DE SEGURIDAD

Para la correcta ejecución se realizará un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúen siendo efectivas e idóneas para la Administración Pública Municipal.

A continuación, se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

Mecanismos de monitoreo.	Objetivo del monitoreo.
Realizar visitas de verificación a cada una de las áreas cada mes.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Solicitar reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.
Aplicar cuestionario sobre protección de datos personales	Constar que el tratamiento de datos personales es adecuado, eficiente y eficaz.

De las medidas de seguridad que aun falten por implementar se realizará un análisis para determinar el tiempo promedio para ser subsanadas, tales adecuaciones se sujetaran, en el caso que requerir la erogación de recursos económicos, a las previsiones presupuestarias existentes, las medidas que no requieran la erogación de recursos deberán ser implementadas a cargo del Auxiliar Administrativo Especializado en Protección de Datos Personales, la Unidad de Transparencia y el Comité de Transparencia, para lo que todas las áreas administrativas deberán prestarles las facilidades necesarias para implementación, vigilancia y evaluación de las medidas de seguridad implementadas y de las necesarias por implementar al interior de la institución, incluso la actualización del presente Documento de Seguridad para la Protección de Datos Personales en la Administración Pública Municipal de Atitalaquia, Hidalgo.

CONCLUSIONES.

Derivado de la elaboración del presente documento, se tiene el propósito de tener una mejora continua, actuar, planificar, verificar y hacer.

Es así que el presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad,
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y
V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte de los usuarios, servidores públicos y del propio Instituto de Transparencia, Acceso a la Información y

Protección de Datos del Estado de Hidalgo, para la mejora del documento de seguridad.

Este instrumento, busca dar certidumbre en el manejo y tratamiento de datos personales, por tanto, no es un producto acabado, es perfectible, sujeto a constante revisión y por tanto actualización y mejora, debiendo estar alienado a la normativa municipal para; cualquier sugerencia puede remitir sus observaciones a la Unidad Municipal de Transparencia y Acceso a la Información del municipio de Atitalaquia, Hidalgo a la siguiente referencia:

UNIDAD DE TRANSPARENCIA
ATITALAQUIA, HIDALGO
2024-2027

Unidad Municipal de Transparencia y Acceso a la Información de Atitalaquia, Hidalgo
Ubicado en Palacio Municipal de Atitalaquia
Col. Centro,
Planta alta, Unidad de Transparencia.
Titular: Mtro. José Edgardo León García
Correo Electrónico: transparencia@atitalaquia.gob.mx